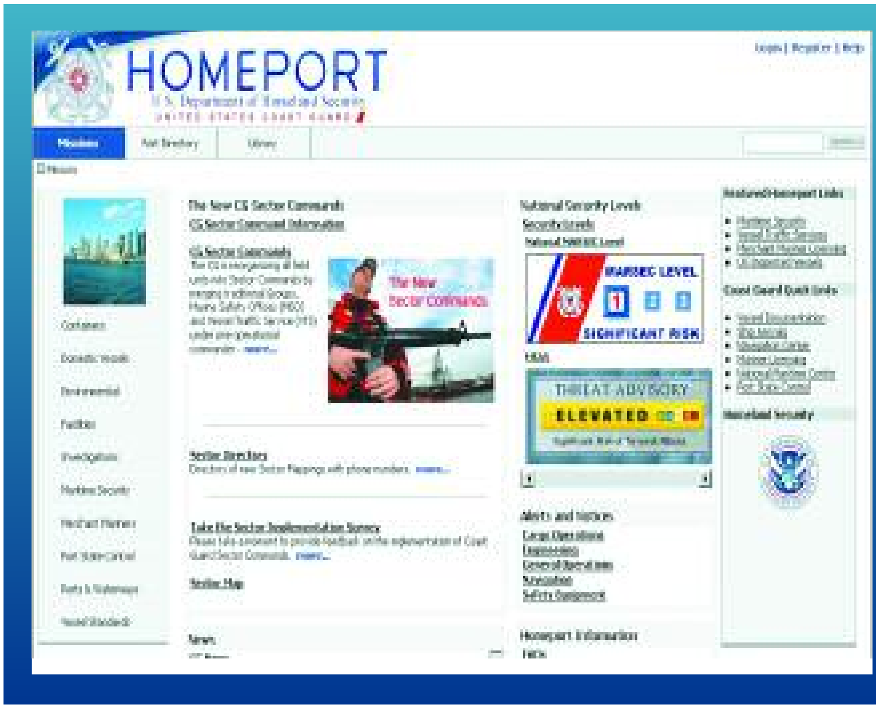
HOMEPORT

This secure Internet portal provides critical information and service to the public, maritime security partners, and Team Coast Guard.

by LCDR Mark Hammond
U.S. Coast Guard Office of Port and Facility Activities

by LCDR Karrie Trebbe
Homeport Project Officer, U.S. Coast Guard Office of Resources and Information for Prevention



Consider these scenarios: An urgent message arrives at the local Captain of the Port office. It requires the immediate dissemination of a Department of Homeland Security threat bulletin containing sensitive security information to all Maritime Transportation Security Act-regulated bulk-liquid facilities in that port. How is this currently accomplished? Multiple phone calls, faxes, hand delivery?

Prior to the next meeting of your Area Maritime Security (AMS) committee, you wish to communicate with committee members, exchange ideas, and solicit comments/feedback regarding a sensitive portion of the AMS plan. However, there is currently no easily accessible, secure method of doing this without meeting face to face.

What about changes in the Maritime Security (MARSEC) level for your port? What is the process by which you ensure appropriate entities are notified in a timely manner, and how do you track MARSEC level attainment for each entity?

Got Homeport? Then no problem!

Homeport (http://homeport.uscg.mil) is a publicly accessible, secure Internet portal that supports unique U.S. Coast Guard business requirements by providing personalized information delivery and critical services to the public, maritime industry, and Team Coast Guard. Version 1.0, which primarily supports port security functionality, was deployed October 3, 2005. It serves as the Coast Guard's primary communication tool to support the sharing, collection, and dissemination of sensitive but unclassified (SBU) information, including sensitive security information (SSI). Homeport delivers an unprecedented level of collaboration and information sharing capability and has the potential to revolutionize the way the Coast Guard communicates with the public and maritime security partners.

Background/History

The Maritime Transportation Security Act of 2002 (MTSA) mandated increased information sharing and the development of a suite of maritime security plans. In light of these requirements, in the spring of 2004, the U.S. Coast Guard Office of Port, Vessel, and Facility Security (G-PCP) sought to develop an electronic plans (e-plans) management system to establish an SSI-level database and Web-based portal access to the vessel, facility, and area maritime security plans required by the MTSA. The proposed concept was to design a system that would afford instant access, within a secure environment, for information sharing and collaboration among critical decision makers within federal, state, local, and industry for routine maritime security and crisis situation management.

The U.S. Coast Guard Office of Information Resources for Prevention collaborated with the Office of Port, Vessel, and Facility Security to develop the proposed system. The Office of Information Resources, in close coordination with the Coast Guard's Infrastructure Management Division and the technical staff at the Coast Guard's Operational Systems Command (OSC), developed a robust, Coast Guard-wide Internet portal. This system also has the potential to replace every Captain of the Port /Federal Maritime Security Coordinator Internet Website and other Coast Guard Websites with one consistent Internet presence.

The capabilities of Homeport also enable the Coast Guard to align with Department of Homeland Security (DHS) goals and support two key points of Secretary Chertoff's six-point agenda:

- increasing overall preparedness, particularly for catastrophic events by enabling wide dissemination of threat/MARSEC information to our maritime stakeholders, and
- enhancing information sharing with our partners.

Further, Homeport serves to support the National Strategy for Homeland Security, released September 2005. This strategy specifies that the federal government will build a national environment that enables the sharing of essential homeland security information horizontally across each agency of the federal government and vertically among federal, state, and local governments; private industry; and citizens. This strategy calls on DHS to lead the effort to define sharing requirements; establish processes for providing and receiving information; and develop technical systems to share sensitive information with public-private stakeholders.

System Development

During the summer of 2004, Homeport was developed and successfully completed DHS vulnerability testing. In November 2004 a prototype of Homeport was initially deployed to eight Coast Guard units for operational testing and evaluation. Development continued and enhancements were made based on user feedback. Operational testing and evaluation was completed in March 2005. Between March 2005 and the official deployment on October 3, 2005, policy and guidance regarding the use of Homeport were developed.

The full capabilities and potential of Homeport were realized during Hurricane Katrina response and recovery operations. Coast Guard operation centers were inundated with phone calls and requests for assistance. In coordination with OSC; the Office of Information Resources; Coast Guard's Infrastructure Management Division; Coast Guard Headquarters Command Center; and the Eighth District Command Center, Homeport developers delivered the capability of allowing the public to complete a missing/stranded person request form online. Coast Guard Headquarters and District Eight operation centers were able to log into Homeport to view the requests. Within 24 hours of making the online request form available, over 6,000 requests were submitted. In the end, Homeport received over 16,000 requests for help.

System Deployment

Multiple training sessions were conducted in July and August 2005 at OSC Martinsburg, W.Va., to establish a pool of qualified Homeport registration approvers. Approvers are responsible for the review, proper vetting, and approval of Homeport user accounts. The training included basic system operations, specific functionality, and key features enabling members to return to their units to begin generating port-wide usage and populating local content areas.

Post-deployment training is planned during fiscal year 2006, consisting of several train-the-trainer sessions. Additionally, on-demand training will be made available to each sector desiring specific, focused training. G-PCP is also in the process of developing a series of training videos that will be available to the field in the near future. These videos will highlight the many useful tools and functionality within the system that are designed to enhance coordination among various port security partners.

G-PCP hosted a series of workshops comprised of Coast Guard personnel, representing a cross section of various field units and program offices. This group was brought together to represent the diversity of potential Homeport users and to address concerns regarding the implementation of Homeport. The end-product of these workshops was G-MPS (now G-PCP) Policy Letter 01-05, which provides detailed guidance on the proper use of the port security functions within Homeport, including review/approval of user registrations, use of SBU communities, publishing threat products, and setting MARSEC levels. A core aspect of the policy that is central to the registration process is the proper vetting of registrants by account approvers, since registered users have access to a variety of sensitive security information.

Access to Homeport user accounts is currently limited to the following user groups:

- owners and operators, vessel security officers, and company security officers of vessels that are required to submit a vessel security plan under MTSA;
- owners, operators, and facility security officers of waterfront facilities required to submit a facility security plan under MTSA;
- members of an Area Maritime Security Committee;
- members of national-level committees, such as the Safety Advisory Committee, Harbor Safety Advisory Committee, National Industry Security Partner, Port Readiness Committee, and National Maritime Security Advisory Committee; and
- Coast Guard members who deal with Area Maritime Security Committees.

User access is approved based on a registrant's eligibility and need to know. The general public has the ability to view a wide range of information, much of which is currently found on the existing Coast Guard Website.

System Capabilities and Features

Homeport Version 1.0 offers many useful capabilities and features for information sharing and collaboration. Anyone can access general information without an account. However, depending on their profile, registered users have access to the following capabilities in Homeport:

- publish and update unit Internet information (such as statistics, safety and security zones, and inspection schedules);
- notify any maritime industry Homeport user (via e-mail);
- change MARSEC levels for the entire COTP zone or an individual port component;
- see MARSEC attainment levels of individual vessels and facilities in their COTP zone;
- view the security plan for any vessel or facility;
- manage Homeport registration for maritime industry users and industry partners;
- manage the security plan review and approval process;
- publish and disseminate local security alerts; review national security alerts and threat products; and collaborate with their Area Maritime Security Committee, Harbor Safety Committees, and Safety Advisory Committees;
- easily publish and maintain enterprise marine safety, security, and environmental protection Internet information;
- publish and disseminate national security alerts;
- publish and disseminate threat products, with the ability to target distribution to specific port users;
- view security plans for any vessel or facility;
- see MARSEC levels of any vessel or facility;
- collaborate with any Area Maritime Security Committee, Harbor Safety Committees, and Safety Advisory Committees or other established communities.

The collaboration feature is one of the most valuable tools of Homeport. Homeport collaboration spaces, known as communities, are where a designated group of users can work together on projects, set meetings, generate tasking, and exchange information about topics of interest within a secure or non-secure environment.

Short-term enhancement plans for Homeport include the incorporation of an enterprise solution for an Alert Notification System (ANS) whereby Captains of the Port and Federal Maritime Security Coordinators can broadcast alerts through multiple means of communication. Further, the office of Information Resources continues to work with DHS on building appropriate connections between Homeport and DHS' Homeland Security Information Network, which provides the main communication, analysis, and collaboration tool for connectivity to state and local agencies.

For more information regarding Homeport, visit http://Homeport.uscg.mil.

About the authors: *LCDR Mark Hammond is stationed at the U.S. Coast Guard Office of Port and Facility Activities.*

LCDR Karrie Trebbe is the Homeport Project Officer, U.S. Coast Guard Office of Resources and Information for Prevention.